IEEE SA
STANDARDS ASSOCIATION

INDUSTRY CONNECTIONS
WHITE PAPER

IEEE 3D BODY PROCESSING INDUSTRY CONNECTIONS (3DBP IC): COMMUNICATION, SECURITY, AND PRIVACY

Authored by

Randy K Rannow, Silverdraft Supercomputing

Alfredo Ballester, Instituto de Biomecánica, Universitat Politècnica de València

Emma Scott, Fashion Should Empower

Carol McDonald, Gneiss Concept

IEEE

3 Park Avenue | New York, NY 10016-5997 | USA

IEEE 3D Body Processing Industry Connections (3DBP IC): Communication, Security, and Privacy

Authors:

Randy K Rannow, *Silverdraft Supercomputing*

Alfredo Ballester, *Instituto de Biomecánica, Universistat Politècnica de València*

Emma Scott, *Fashion Should Empower*

Carol McDonald, *Gneiss Concept*

Acknowledgments

The ideas in this paper are a collaborative result of many conversations of the 3DBP IC group, as well as discussions with closely aligned professionals. The authors acknowledge the individual members of the 3DBP IC for their valuable feedback and encouragement.

Trademarks and Disclaimers

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-1-5044-6178-8 STDVA23901

To order IEEE Press Publications, call 1-800-678-IEEE.
Find IEEE standards and standards-related product listings at: http://standards.ieee.org

Notice and Disclaimer of Liability
Concerning the Use of IEEE SA Industry Connections Documents

This IEEE Standards Association ("IEEE SA") Industry Connections publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE SA Industry Connections activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE SA Industry Connections document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at http://standards.ieee.org/about/sasb/iccom/.

This Work is published with the understanding that IEEE and the IEEE SA Industry Connections activity members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

Contents

IEEE 3D Body Processing Industry Connections (3DBP IC): Communication, Security, and Privacy

Abstract

The 3DBP IC Communications, Security and Privacy (CSP) subgroup is investigating the protection of data and records that may contain personal information, and how to ensure users and consumers expectations relative to privacy and security. The subgroup has determined that the requirements from the IEEE draft standards of P7002, P7004, and P7012 can be applied to 3DBP to help ensure security and privacy. Furthermore, it appears existing standards and industry practices will be helpful to enable the CSP to create requirements as normative clauses in a standard, and will use the existing standards, to the extent possible, to help enable safe, secure, transparent, and private processing of 3DBP information. In addition, the global impact of the EU GDPR will have a rippling influence on privacy requirements and the CSP is further assessing GDPR relative to data and record exchange in terms of privacy and security.

1. Introduction

The 3DBP IC is a body of individuals that is collaboratively assessing aspects of 3D body processing technologies, as well as the exchange or interchange and implementation or use of anthropometric data that may be used in the apparel and other industries and sectors, and to help facilitate the IEEE P3141 working group to move forward creating a standard for the secure interoperability and deployment of 3D body processing technologies. The 3DBP IC created a Communication, Security, and Privacy (CSP) subgroup to further assess the transmission, storage, and use of data—information that contains detailed anthropometric facts. The secure communication or transmission of this privileged or private information is a key consideration. What mechanisms can impact, influence, or contribute to secure transmission or data sharing, and as devices become increasingly connected, how can privacy and security be should also be considered.

Background

Today's computing systems suffer from the dichotomy between computation/processing and data storage. Due to this dichotomy, data is nearly always moving, and being stored, in order for the system to perform computation on it. With 3D body processing, scans of individuals are obtained using fixed or mobile technologies, single cameras or multiple cameras, RF or photonics, static or dynamic. Advances in 3D imaging technologies has enabled human shape databases. Generating human shape from traditional anthropometric measurement methods is becoming mainstream. At the same time, we know that various 3D body processing approaches are not new, with similar schemes used for airport security and MRIs. A data-rich survey on research challenges, solutions, and deployments of 3D body processing are discussed in past Proceeding of the 3D Body Tech Conference. These surveys, may not capture details related to

commercialization, standardization, imaging, and CSP, as well as how new mobile devices and their communication or connectivity may influence 3D body processing. To fully realize the potential influence, diligence in these aspects relative to 3D body processing necessitates a CSP taxonomy as illustrated in Figure 1.

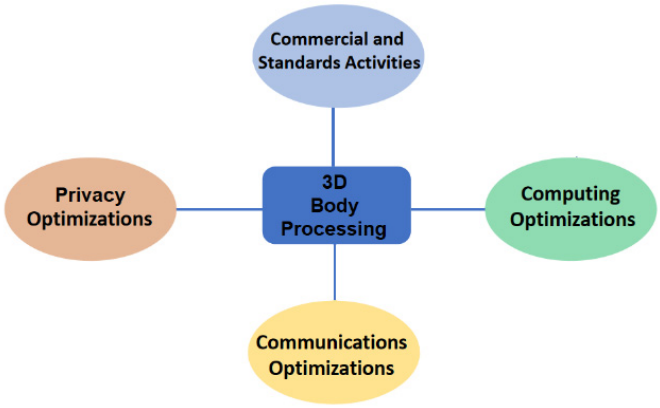


Figure 1 —CSP taxonomy

GDPR

On 25 May 2018, The European Union (EU) implemented a privacy requirement intended to strengthen and unify a consistent personal data privacy and protection regime within the EU: General Data Protection Regulation (GDPR). Personal data is defined as any information relating to an individual that can be used to directly or indirectly identify an individual. In essence, GDPR aims at giving back to individuals the full control of their personal data. GDPR is not much different from prior legislation, however, it emphasizes much more on its enforcement. GDPR applies to companies or entities that collect and handle personal data from EU-based individuals, regardless of where the data is processed. Since 3D body processing can include personal data, GDPR applies accordingly.

2. Communication, security, and privacy (CSP)

CSP are three distinct and fundamental attributes associated with the interoperability and interchange of detailed anthropometric data in 3D body processing. While separate matters, they are inter-related, and therefore must be thoroughly vetted for pragmatic purposes.

Communication

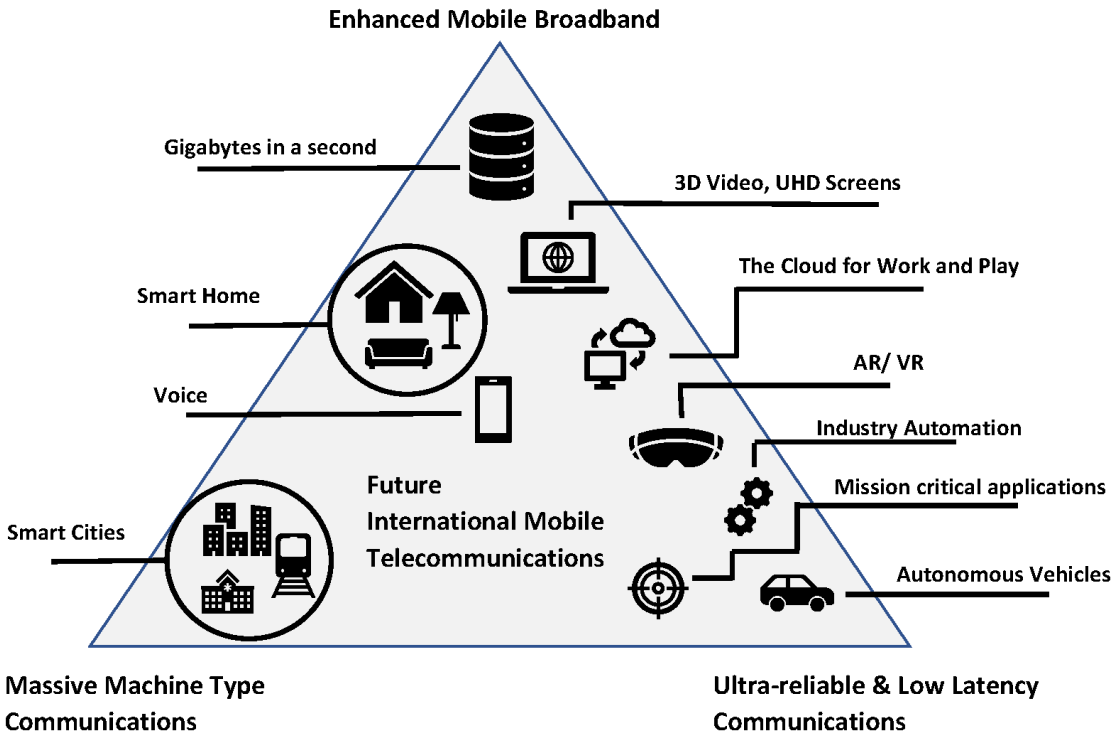
Communication in 3DBP includes the connectivity as the infrastructure, as well as the protocols involved in the transmission of digitized records or data between two or more devices or locations. Computer communications for 3DBP includes the process in which exchange of information using networked or connected devices is realized. 3DBP communication may also include a network in which any number of independent devices or computers are interconnected for data exchange. These networks are established to transfer information or data from one device or system to another, or to share resources.

Over the past few years, there has been a radical shift toward always connected devices; always connected has improved efficiency. Ubiquitous connectivity makes devices vulnerable to unauthorized access, susceptible to cyber threats. These vulnerabilities or threats include malware, phishing, web-based and application-based attacks, spam, ransomware, data breaches, denial of service, information leakage, etc. To help mitigate these issues, 3DBP is evaluating and interfacing with networking entities, such as the IEEE 802 LMSC (LAN/MAN Standards Committee), who in-turn work with global entities, focused primarily on the lowest two layers of the ISO Reference Model for Open Systems Interconnection (OSI). The IEEE 802 LMSC includes Working Groups (WG) and Technical Advisory Groups (TAG):

- IEEE 802.1 High Level Interface (HILI) Working Group
- IEEE 802.3 CSMA/CD (Ethernet) Working Group
- IEEE802.11 Wireless LAN (WLAN) Working Group
- IEEE 802.15 Wireless Personal Area Network (WPAN) Working Group
- IEEE 802.16 Broadband Wireless Access (BWA) Working Group
- IEEE 802.17 Resilient Packet Ring (RPR) Working Group
- IEEE 802.18 Radio Regulatory Technical Advisory Group
- IEEE 802.19 Coexistence Technical Advisory Group
- IEEE 802.20 Mobile Broadband Wireless Access Working Group
- IEEE 802.21 Media Independent Handover Working Group
- IEEE 802.22 Wireless Regional Area Networks (RAN) Working Group
- IEEE 802.24 Technical Advisory Group

As the entity or group titles indicate, these individuals are well versed in communications. Additionally, the IEEE 802 LMSC has formal and informal liaison and external communications with global organizations to help ensure interoperability, as well as functional communication and operation. In the case of wide area networks (WAN), these extend over large geographic areas (e.g., countries or continents), or used by internet service providers to connect local companies or users to the internet. Personal area networks (body networks), to intercontinental communications are activities with which IEEE continues to engage. The 3DBP CSP is leveraging, to the extent possible, the work by the IEEE 802 LMSC and the IEEE, including ISO/IEC/IEEE 15288 due to their ongoing activities directly related to future communications and networks, especially as next generation networks and quantum computing evolve.

With increasing exchange of data, communications will require even higher bandwidths and ultra-low latency, and with the continued proliferation of portable devices used in 3DBP, lower power requirements for next generation of solutions will always be a priority. Furthermore, the collaborative standards development within the IEEE SA includes adjacent activities, such as standards for digital media, immersive visual content, and 3D medical simulation. Figure 2 illustrates capacity, connectivity, and reliability for communications that are potential enablers for 3DBP going forward.



Adapted from ITU by Gneiss Concept and reprinted with Gneiss Concept's permission

Figure 2 —Potential enablers for 3DBP in the future

Security

Security for the 3DBP is another key triad attribute being considered by the CSP subgroup. Smart connectivity and ubiquitous computing will pave the way for billions of highly-functional devices that can communicate with another device or other devices with minimal or no human involvement. The potential magnitude of the deployment of 3DBP solutions may require scenarios of intentionally disconnecting from a communication network.

The Association of Computing Machinery (ACM) SIGMETRICS group is an ACM Special Interest Group for the computer systems performance evaluation community. The ACM also has an ongoing annual International Conferences on Security of Information and Networks (SIN), an event first started in 2007. SIN is a forum where global participants share research and applications of communication and computer security in information, networks, and systems. The ACM has focused groups working on various information security or communication security. The 3DBP CSP subgroup commenced a comprehensive survey of device and computer security that may be used in 3DBP. This analysis includes security concepts, methods, and practices of potential principles and practices for 3DBP devices, systems, or solutions. Network security tools, policies, and administrative objectives are matters being addressed by the CSP. Based on a review of ACM's SIGSAC (Special Interest Group on Security, Audit, and Control) activities, as well as papers and presentations from their annual conference on Data and Application Security and Privacy, the CSP subgroup recognizes that the need for security continues to grow with distributed computing devices that may be used in 3DBP. Conventional

security monitoring and analytic solutions are typically signature-based tools that identify threats that have been previously observed or experienced [1], [2]. Based on the 3DBP solutions survey, security will need to include generated data (training information), as well as inference processes (decision-making) that can be realized using machine learning (ML) or deep learning (DL) algorithms. Furthermore, a multi-layer threat and vulnerability analysis approach using generated data, as well as network traffic and user interaction may be part of the approach specified in IEEE P3141, Draft Standard for 3D Body Processing.

The IEEE Computer Society's Technical Committee on Security and Privacy (TCSP) is another entity with which the 3DBP group is collaborating. The TSCP is engaged in subjects related to operating system security, data encryption, mechanisms for access control, database safeguards, and information security. The IEEE Cybersecurity and Privacy Standards Committee is responsible for standards on cybersecurity and privacy. The IEEE organizationally has a number of resources that are being reviewed and included as the 3DBP develops recommendations for IEEE P3141 security aspects.

For the CSP subgroup, intrusion detection solutions are defined as systems or tools built to monitor and analyze network communications, and detect anomalies or unauthorized intrusions into devices or systems used for 3DBP. With ML and DL being deployed as intrusion detection solutions (IDS), the CSP subgroup will include an IDS approach that may utilize algorithms for assessing general attributes characterizing the intrusion, decision-making features, assessment metrics, intrusion location, triggers, and actions. To the extent possible, security considerations will include active and passive threats or potential threats, and be designed to be agile, and therefore able to adapt to the constant changes in attacks and network architectures.

With a growing concern on security and privacy, having the resources to help ensure compliance with any requirement may force academic aspects to be addressed in terms of trained information security experts. Such is the hypothesis of a paper by a collaborative group in the United Kingdom [5] where the authors discuss aspects of formally educating individuals in cyber security.

Based on research and analysis of 3DBP technologies and solutions, the CSP subgroup will work to ensure secure networks are used for data and information exchange. Their activities will also work to reduce security vulnerabilities, deploy or require automation and other processes as effective and efficient security tools, and recommend or require processes and procedures in place to improve collection and analysis of data [3], [4].

Privacy

While working on privacy, another key CSP triplet attribute, tthe 3DBP CSP subgroup has come to the realization that a concise definition may be lacking and thus recognizes that a common or foundational description is prudent. In making the 3DBP recommendations to the IEEE P3141 working group, privacy will be an ad hoc definition as it relates to 3D body processing and the sharing or exchange of information. Anthropometric privacy, communication privacy, information privacy, and individual privacy will include the collection of handling of personal data, where personal data is any descriptive information relating to an individual or particular person.

Over the past ten years, social network platforms have attracted billions of users, with billions of smart devices connected to the internet. Cumulative data from The Fashion and Apparel Industry Report [6] shows global revenue may grow from nearly $481B in 2018 to $713B by 2022, with potential CAGRs of 8.5% (US and Europe) and 14% (China) over this same period. Figure 3 reflects data from Statista.

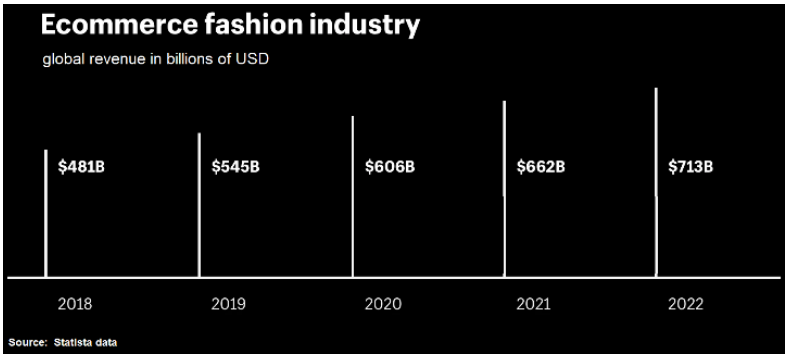


Figure 3 —Global revenue chart

The emergence of electronic medical records provides a convenient approach for the exchange or sharing of personal data, especially as the move to store data electronically grows in the medical arena. Privacy is mandated for the electronic sharing and blockchain is one potential solution being considered by this sector. It appears that perhaps part of the privacy solution may be the implementation of blockchain technology as the process of information or data exchange in 3DBP is to enable better collaboration, improved customer experience, and the ledger functionality of blockchain, as well as the distributed-decentralized database enables digital information to be stored at different locations. The blockchain network includes several nodes operating in a peer-to-peer manner with each node relaying to each other (vs. a central authority). For the nodes in the network, consensus algorithms validate the set of transactions gathered blocks. The application of blockchain technology may enable benefits on trust enhancement, peer-to-peer data exchange, non-repudiation, data security and integrity, and auditing. Because medical information has specific information security and privacy protection requirements, blockchain technology may be a viable tool for data integrity protection for 3DBP, and investigation of this technology continues. In this sense, BODYPASS, an EU co-funded project [9], is exploring and implementing a blockchain network to cope with needs for 3D body data trade between fashion and the apparel industry and the healthcare sector while coping with the aforementioned security and privacy challenges [10].

The IEEE commenced a formal ethics in action activity as part of an IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems with the motivation to move from principles to practice. The IEEE P7000™ Standards Projects [7] include the following:

- IEEE P7000™, Draft Model Process for Addressing Ethical Concerns During System Design
- IEEE P7001™, Draft Transparency of Autonomous Systems
- IEEE P7002™, Draft Data Privacy Process
- IEEE P7003™, Draft Algorithm Bias Considerations

- IEEE P7004™, Draft Standard on Child and Student Data Governance
- IEEE P7005™, Draft Standard on Employer Data Governance
- IEEE P7006™, Draft Standard on Personal Data AI Agent Working Group
- IEEE P7007™, Draft Ontological Standard for Ethically driven Robotics and Automation Systems
- IEEE P7008™, Draft Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems
- IEEE P7009™, Draft Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems
- IEEE P7010™, Draft Wellbeing Metrics Standard for Ethical Artificial Intelligence and Autonomous Systems
- IEEE P7011™, Draft Process of Identifying and Rating the Trustworthiness of News Sources
- IEEE P7012™, Draft Standard for Machine Readable Personal Privacy Terms
- IEEE P7013™, Draft Inclusion and Application Standards for Automated Facial Analysis Technology
- IEEE P7014™, Draft Standard for Ethical Considerations in Emulated Empathy in Autonomous and Intelligent Systems

While all these standards may not be sufficiently specific or applicable to 3DBP, at this point the CSP subgroup is focused on leveraging IEEE P7002 since this standard is defining requirements for engineering processes for privacy oriented considerations as it relates to products, services, and systems, as well as including privacy practices and privacy impact assessments. IEEE P7004 and IEEE P7005 also have relevant requirements and will be included, as appropriate, in the recommendations from 3DBP to IEEE P3141. Through information liaison with the IEEE P7002 leadership, the 3DBP has suggested that an addendum to IEEE P7002 may be an appropriate mechanism to help ensure application or use specific requirements, including normative items, can be formally standardized with normative clauses.

The CSP subgroup has also analyzed how work related to e-voting standards and practices may be leveraged. The development of e-voting or electronic voting systems is an important direction of work due to the ubiquitous transfer of paper to the information technology operating environment. The premise is that e-voting, in comparison with traditional processes, may enable lower cost, more reliable, and perhaps greater convenience. Regardless of these ideas, privacy, security, and traceability is perhaps paramount for e-voting, attributes that are also key for 3DBP information sharing and exchange for privacy-related matters or purposes.

The 1986 Electronic Communications Privacy Act (ECPA) [8] called for the expansion and revision of federal wiretapping and electronic eavesdropping provisions. It was enacted to promote “the privacy expectations of citizens and the legitimate needs of law enforcement.” The US Congress also sought to support the creation of new technologies by assuring consumers that their personal information would remain safe.

ECPA included amendments to the Wiretap Act, created the Stored Communications Act, and created the Pen Register Act. The Wiretap Act concerns interception of electronic and wire communications, which include “any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection.” An oral communication is “any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.” This constitutes any oral conversation in person where there is the expectation that no third party is listening. While not inclusive to the extent necessary for today’s 3DBP privacy, it is a regulatory requirement in the United States that the CSP subgroup will include in its recommendations for the 3DBP group.

3. Communication, security, privacy summary

There are three key attributes associated with the interoperability and interchange of detailed anthropometric data that is or may be used as part of 3D body processing. While distinct topics, they are inter-related, and are be systematically investigated for pragmatic purposes, and how they may apply to IEEE P3141. Existing standards and practices will be leveraged, and regulatory requirements (e.g., USC and GDPR) will be the precedent setting requirements, the 3DBP recommendations will encompass and define those requirements necessary to help ensure an appropriate standard.

Citations

[1] H. Jiang, G. Zhang, G. Xie, K. Salamatian, and L. Mathy, “Scalable high performance parallel design for network intrusion detection systems on many-core processors,” in Proc. IEEE ANCS, 2013.

[2] H. Gill, D. Lin, X. Han, C. Nguyen, T. Gill, and B. T. Loo, “Scalanytics: A declarative multi-core platform for scalable composable traffic analytics,” in Proceedings of the 22Nd International Symposium on High performance Parallel and Distributed Computing, ser. HPDC ’13.New York, NY, USA: ACM, 2013, pp. 61–72

[3] https://www.thesslstore.com/blog/the-top-cyber-security-trends-in-2019-and-what-to-expect-in-2020/

[4] https://www.symantec.com/security-center/threat-report

[5] Davenport, J., Crick, T., Irons, A., & Prickett, T. (Accepted/In press). A UK Case Study on Cybersecurity Education and Accreditation. In Frontiers in Education 2019 (IEEE Frontiers in Education Conference). IEEE.

[6] https://www.shopify.com/plus/industry-reports/fashion-and-apparel?itcat=plusblog&itterm=ecommerce-fashion-industry

[7] https://ethicsinaction.ieee.org/

[8] https://www.govinfo.gov/app/details/USCODE-2011-title18/USCODE-2011-title18-partI-chap119

[9] BODYPASS Project: API-ecosystem for cross-sectorial exchange of 3D personal data. Supported by European Union’s Horizon 2020 research and innovation program under grant agreement No 779780

[10] Dura, J. V. (2019). BODYPASS: The interoperability challenges of 3D personal data. Presented at the BDVA PPP SUMMIT, Riga. Retrieved from https://es.slideshare.net/JuanVDura/the-interoperability-challenges-of-3d-personal-data

IEEE SA
STANDARDS ASSOCIATION

RAISING THE WORLD'S STANDARDS

Connect with us on:

Twitter: twitter.com/ieeesa
Facebook: facebook.com/ieeesa
LinkedIn: linkedin.com/groups/1791118
Beyond Standards blog: beyondstandards.ieee.org
YouTube: youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060

IEEE